(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Numéro de publication: **0 671 712 A1**

(12) DEMANDE DE BREVET EUROPEEN

(21) Numéro de dépôt: **95400505.4**

(51) Int. Cl.[6]: **G07F 7/08**

(22) Date de dépôt: **09.03.95**

(30) Priorité: **09.03.94 FR 9402717**

(43) Date de publication de la demande:
13.09.95 Bulletin 95/37

(84) Etats contractants désignés:
AT BE CH DE DK ES FR GB GR IE IT LI LU NL PT SE

(71) Demandeur: **BULL CP8**
68 route de Versailles,
B.P. 45
F-78430 Louveciennes (FR)

(72) Inventeur: **Patarin, Jacques**
11 rue Amédée Dailly
F-78220 Viroflay (FR)

(74) Mandataire: **Corlu, Bernard et al**
Direction de la Propriété Intellectuelle BULL SA,
Poste Courrier: LV59C18,
68 route de Versailles,
B.P. 45
F-78430 Louveciennes (FR)

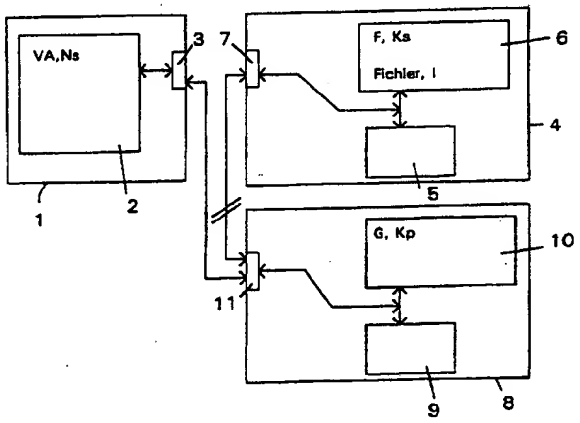
(54) Procédé et dispositif pour authentifier un support de données destiné à permettre une transaction ou l'accès à un service ou à un lieu, et support correspondant.

(57) L'invention concerne un procédé et un dispositif pour authentifier un support de données destiné à permettre une transaction ou l'accès à un service ou à un lieu, et le support correspondant.

Selon l'invention, le support (1) porte un numéro propre (Ns) et une valeur d'authentification calculée au moyen d'un algorithme dissymétrique (F) et d'une clé secrète (Ks), à partir du numéro propre et d'une information (I) définissant les droits attachés au support.

On prévoit deux types d'authentification, l'une courante, en mode déconnecté de l'organisme habilité, l'autre périodique, en mode connecté. En mode déconnecté, on applique à la valeur d'authentification (VA) lue sur le support un algorithme (G) corrélé à l'algorithme dissymétrique (F) et utilisant une clé publique (Kp) pour vérifier d'une part que la valeur d'authentification (VA) est compatible avec le numéro propre (Ns) et l'information (I), et d'autre part que la transaction ou le service demandé est compatible avec l'information (I).

En mode connecté, il est en outre possible de modifier la valeur d'authentification du support.



EP 0 671 712 A1

L'invention concerne un procédé pour authentifier un support de données ou un dispositif comme émanant bien d'un organisme habilité, ce support ou dispositif étant destiné à effectuer des transactions ou à permettre l'accès à un service ou à un lieu auprès d'un distributeur affilié audit organisme, l'organisme détenant, dans un fichier, le contenu des droits actuels attachés à chaque support, procédé consistant à attribuer audit support un numéro propre (Ns) permettant de le distinguer parmi un ensemble de supports produits par ledit organisme, et à porter ce numéro sur le support.

Le but de l'invention est de proposer un procédé de ce genre qui mette en oeuvre les moyens les plus simples dans le support lui-même et dans un éventuel terminal du distributeur destiné à coopérer avec le support. Dans le cas par exemple où le support est électronique, on souhaite qu'il soit constitué seulement par une mémoire, à l'exclusion de circuits de calcul associés, et que cette mémoire ait une taille la plus faible possible. On souhaite également que ni le support, ni le terminal associé ne renferme de clé secrète, une telle clé étant susceptible d'être découverte par un fraudeur.

Selon l'invention, ces buts sont atteints grâce à un procédé du genre cité au début de l'exposé, et consistant en outre à initialiser ledit support ou dispositif chez l'organisme en lui attribuant une information (I) définissant, en fonction du contenu dudit fichier, les droits attachés à ce support, en calculant, à partir du numéro propre (Ns) et de l'information (I), une valeur d'authentification (VA) au moyen d'un algorithme dissymétrique (F) et d'une clé secrète (Ks), et en portant cette valeur d'authentification sur le support ; à procéder, lors de chaque utilisation du support, à une authentification de celui-ci par ledit distributeur dans un mode non connecté à l'organisme habilité, en effectuant un calcul par application à un algorithme (G) corrélé audit algorithme dissymétrique (F), d'une clé publique (Kp) associée à ladite clé secrète (Ks) et de la valeur d'authentification (VA) lue sur le support pour vérifier d'une part que la valeur d'authentification (VA) est compatible avec le numéro propre (Ns) et l'information (I), et d'autre part que la transaction ou le service demandé est compatible avec l'information (I) ; à procéder périodiquement ou en fonction du type de transaction ou service, à une authentification du support à partir du distributeur dans un mode connecté à l'organisme habilité en effectuant tout d'abord une authentification du support par le distributeur ou l'organisme habilité qui vérifie que la valeur d'authentification (VA) lue sur le support est compatible avec le numéro propre (Ns) et l'information (I) et, si l'authentification est positive, en faisant confirmer par l'organisme habilité que le support possède encore des droits en fonction de l'état actuel dudit fichier puis, dans l'affirmative et si un changement de l'information (I) est nécessaire pour traduire l'état actuel des droits, en calculant, à partir du numéro propre (Ns) et d'une nouvelle information (I), une nouvelle valeur d'authentification (VA') au moyen de l'algorithme dissymétrique (F) et de la clé secrète (Ks), et en portant cette nouvelle valeur sur le support. L'utilisation d'un algorithme dissymétrique permet que seules les opérations d'inscription de la valeur d'authentification (VA) nécessitent l'usage d'une clé secrète, tandis que la vérification habituelle de cette valeur requiert seulement une clé publique.

Cependant, le fait de prévoir une connexion périodique avec l'organisme habilité permet de procéder à une vérification plus complète des droits attachés à chaque support et de mettre à jour si nécessaire le support.

L'invention concerne aussi les différents dispositifs associés au procédé ci-dessus.

D'autres détails et avantages de l'invention apparaîtront au cours de la description suivante d'une forme de réalisation préférée mais non limitative, en regard de la figure unique annexée représentant schématiquement un objet portatif coopérant avec un terminal d'un organisme habilité et un terminal installé sur un lieu de vente.

Sur la figure, on a représenté en 1 un objet portatif, notamment une carte électronique, équipé d'une mémoire EEPROM 2 reliée à l'extérieur par une interface 3. La carte ne comporte pas de circuits de traitement du genre microprocesseur. Dans la mémoire 2, se trouve notamment deux informations, à savoir un numéro de série Ns de la carte, alloué à celle-ci lors de sa fabrication, et une valeur d'authentification VA destinée à prouver que la carte émane bien d'un organisme habilité. Le calcul de la valeur VA sera exposé ci-après.

En 4 est représenté un ordinateur central de l'organisme habilité à émettre ou mettre à jour la carte 1. Il inclut notamment des circuits de traitement 5 et une mémoire 6 communiquant entre eux et avec une interface 7. Dans la mémoire 6, est implanté le programme d'un algorithme cryptographique dissymétrique F qui, de façon connue en soi, nécessite l'usage d'une clé secrète Ks, également en mémoire, pour le chiffrement d'une donnée, tandis que son déchiffrement nécessite seulement l'usage d'une clé publique correspondante Kp. Dans la mémoire 6, se trouve encore un fichier contenant les droits actuels attachés à chacun des supports émanant de l'organisme habilité.

Il s'agit de calculer une valeur d'authentification VA pour l'introduire dans la carte 1, en utilisant deux données, à savoir le numéro de série Ns de la carte et une information I définissant les droits attachés à cette carte. L'information I est élaborée en fonction du contenu du fichier et peut par exem-

ple prendre l'une des formes suivantes :

1. Une date de référence permettant de calculer une date limite des droits : il s'agit notamment de la date à laquelle le titulaire de la carte a souscrit un service donné pour une durée déterminée, ou directement la date limite d'accès à ce service;
2. le message suivant : "N'acceptez aucune transaction d'un montant supérieur à 100 Fr.";
3. le message : "à ce jour, les droits de Mr X sont valables";
4. un chiffre, entre 1 et 10, définissant le degré de confiance que l'organisme a dans le titulaire de la carte.

De préférence, l'information I, qui n'est pas secrète, est néanmoins exprimée sous une forme chiffrée pour préserver une certaine confidentialité.

On peut ainsi écrire :

$$VA = F(Ns, I, Ks)$$

On notera que VA peut être considéré comme une signature dissymétrique d'un message constitué par le numéro de série Ns et l'information I.

En variante, le numéro Ns pourra être constitué par tout autre numéro capable d'identifier individuellement la carte 1.

En 8 est représenté un terminal point de vente pour la distribution de biens ou de services, ou le paiement de ceux-ci. Il comporte des circuits de traitement 9 et une mémoire 10 coopérant entre eux et avec une interface 11 par des liaisons appropriées. La mémoire contient le programme d'un algorithme G associé à l'algorithme précité F et la clé publique Kp associée à la clé secrète Ks.

Selon une première forme de réalisation, on met en oeuvre une procédure du type "with message recovery" (c'est-à-dire permettant de récupérer le contenu du message). Dans ce cas, l'algorithme F est basé sur le problème de la factorisation et l'algorithme G contenu dans le terminal est constitué par l'algorithme (F^{-1}) inverse de l'algorithme F. Pour assurer le caractère sécuritaire du calcul de VA, la dimension de VA dans la mémoire 2 de la carte 1 devra être de préférence au moins égale à 512 bits.

Le terminal est donc apte à retrouver le couple de valeurs Ns, I de la façon suivante :

$$(Ns, I) = F^{-1}(VA, Kp)$$

En tant qu'algorithme F, on peut notamment utiliser un algorithme du type RSA (Rivest, Shamir, Adleman), par exemple sous la forme suivante

$$VA = \sqrt[3]{(Ns,I)} \text{ modulo } n$$

où :

- (Ns, I) représente la concaténation de Ns et I ;
- n représente la clé publique Kp ; $n = p \times q$, p et q étant deux nombres premiers secrets constituant la clé secrète Ks.

Dans ce cas, F^{-1} s'exprime comme suit :

$$(Ns, I) = VA^3 \text{ modulo } n$$

La méthode d'authentification de la carte comprend tout d'abord une phase d'initialisation chez l'organisme habilité où l'ordinateur central 4 de celui-ci calcule une première valeur VA pour une carte donnée et la rentre dans la mémoire 2 de celle-ci.

En utilisation, le termina 8 de chaque point de vente affilié à l'organisme habilité peut procéder, de façon déconnectée par rapport à l'ordinateur central 4 de l'organisme, à un certain nombre de vérifications successives d'une même carte 1, correspondant à autant de transactions demandées. A chaque vérification, il recalcule le couple Ns, I à partir de l'algorithme F^{-1} appliqué à la valeur VA qu'il lit dans la mémoire de la carte. Il peut alors vérifier d'une part que le numéro de série Ns qu'il lit dans la mémoire de la carte correspond bien à celui calculé, d'autre part que l'information I calculée est une information cohérente en soi, c'est-à-dire qu'elle constitue un message compréhensible et qu'elle est compatible avec la transaction demandée. Dans l'affirmative, le terminal point de vente peut autoriser la transaction.

En référence aux numéros des exemples d'informations I donnés précédemment, la vérification de la compatibilité pourra par exemple consister à s'assurer :

1. que la date limite des droits n'est pas dépassée, au jour de la transaction;
2. que le montant de la transaction n'est pas supérieur à 100 Fr.;
3. que les droits de Mr X n'exigent pas une nouvelle confirmation de la part de l'organisme habilité, compte tenu de l'ancienneté de la confirmation précédente;
4. que la nature de la transaction est autorisée, compte tenu du chiffre attribué.

En revanche, une différence entre Ns lu et Ns calculé ou une incohérence de l'information I calculée indiquerait que la carte ne provient pas de l'organisme habilité, de sorte que le terminal point de vente refuserait la transaction.

Une fois par mois par exemple, ou lors de grosses transactions, le terminal point de vente procède à une vérification en mode "connecté" à l'ordinateur central 4 de l'organisme habilité. Dans une première phase, il s'agit de s'assurer que la carte est bien authentique. Cela peut s'effectuer de deux manières. Soit c'est le terminal point de vente

qui vérifie la valeur VA en mode "déconnecté" comme exposé précédemment. Soit c'est l'organisme habilité qui s'en charge : celui-ci possédant tous les éléments lui ayant permis d'attribuer à la carte une valeur d'authentification VA, il lui est aisé de vérifier la valeur VA lue sur la carte, par exemple soit par comparaison directe avec le contenu du fichier dans lequel il aura consigné la valeur VA authentique, le numéro de série Ns et l'information I, soit par comparaison avec une valeur VA recalculée pour la circonstance de la manière décrite plus haut.

Dans une seconde phase, dans laquelle le fonctionnement est dans tous les cas en mode "connecté", l'ordinateur central de l'organisme vérifie, en consultant le fichier, que la carte portant le numéro Ns recalculé possède encore des droits. Il vérifie par exemple :

- qu'une opposition n'a pas été déposée, suite au vol de la carte;
- que le compte bancaire auquel la carte ouvre droit, n'est pas à découvert ;
  etc.

Dans une troisième phase, et en tant que de besoin, l'organisme "rafraîchit" la valeur d'authentification VA pour proroger la limite de validité en fonction des droits existants de la carte, ou en fonction de nouveaux droits souscrits depuis la dernière connexion. Pour ce faire, l'ordinateur central de l'organisme calcule une nouvelle valeur VA' en fonction d'une nouvelle information I' prenant en compte cette modification des droits :

$$VA' = F(Ns, I', Ks)$$

Puis il inscrit cette valeur VA' dans la mémoire 2 de la carte, à la place de la valeur actuelle VA, ce qui clôt la procédure.

Selon une seconde forme de réalisation de l'invention, on met en oeuvre une procédure du type "without message recovery" (c'est-à-dire ne permettant pas de récupérer le contenu du message). Dans ce cas, l'algorithme F est par exemple basé sur le problème du logarithme discret et l'algorithme G contenu dans le termina n'est pas constitué par l'algorithme F^{-1} inverse de F mais est seulement corrélé à celui-ci de façon qu'il permette de vérifier que la valeur d'authentification VA a bien été calculée à partir du numéro de série Ns et de l'information I. L'algorithme G est par exemple l'algorithme connu DSS (Digital Signature Standard) qui permet, à partir de la valeur d'authentification VA, de la clé publique Kp, mais aussi du numéro de série Ns et de l'information I de vérifier la compatibilité entre VA d'une part et Ns, I d'autre part. Ici, le recalcul de Ns et I par le terminal n'est pas possible. En revanche, il suffit, pour assurer le caractère sécuritaire de VA, que la dimension de celle-ci dans la mémoire 2 de la carte 1 soit de préférence au moins égale à 320 bits.

Le calcul de compatibilité par le terminal exige, dans cette seconde forme de réalisation, que celui-ci ait connaissance du numéro de série Ns et de l'information I. En ce qui concerne le numéro de série, il sera lu par le terminal sur la carte 1. Pour ce qui est de l'information I, deux situations sont envisageables :

- soit cette information est stockée dans la mémoire 2 de la carte, et le terminal vient la lire ;
- soit cette information est connue implicitement du terminal parce qu'elle est unique pour toute une catégorie donnée de clients ; il peut s'agir d'une information sous la forme suivante : "transactions admises jusqu'à 1000 Francs".

En utilisation, le terminal 8 de chaque point de vente peut procéder, en mode déconnecté, à des vérifications successives d'une même carte 1. A chaque fois, il vérifie la compatibilité de la valeur VA avec les valeurs Ns, I en utilisant l'algorithme G, ces trois valeurs étant lues sur la carte ou -pour ce qui est de l'information I - connue implicitement du terminal. Dans l'affirmative, il peut autoriser la transaction. Comme dans la première forme de réalisation, le terminal peut vérifier la compatibilité de l'information I avec la transaction demandée.

Le fonctionnement en mode connecté est semblable à celui décrit pour la première forme de réalisation, la seule différence étant que, si la première phase précitée dans laquelle on vérifie l'authenticité de la carte est effectuée par le terminal point de vente, les valeurs Ns et I considérées sont celles lues sur la carte et non plus celles recalculées. Si les droits attachés à la carte doivent être modifiés, l'ordinateur central de l'organisme habilité inscrit une nouvelle valeur d'authentification VA' et, le cas échéant, une nouvelle information I' à la place des données actuelles.

La présente invention s'applique non seulement à l'authentification d'une carte à mémoire, mais plus généralement de tout support de données de type électronique ou non, par exemple de type papier (pièce d'identité ou carte d'habitation sur laquelle sont inscrits le numéro de série Ns et la valeur d'authentification VA).

Le support de données peut même être constitué par un dispositif tel qu'un ordinateur portable incorporant le numéro de série Ns et la valeur d'authentification VA.

Revendications

1. Procédé pour authentifier un support de données ou un dispositif comme émanant bien

d'un organisme habilité, ce support ou dispositif étant destiné à effectuer des transactions ou à permettre l'accès à un service ou à un lieu auprès d'un distributeur affilié audit organisme, l'organisme détenant, dans un fichier, le contenu des droits actuels attachés à chaque support, procédé consistant à attribuer audit support un numéro propre (Ns) permettant de le distinguer parmi un ensemble de supports produits par ledit organisme, et à porter ce numéro sur le support, caractérisé en ce qu'il consiste en outre a :

- initialiser ledit support ou dispositif chez l'organisme en lui attribuant une information (I) définissant, en fonction du contenu dudit fichier, les droits attachés à ce support, en calculant, à partir du numéro propre (Ns) et de l'information (I), une valeur d'authentification (VA) au moyen d'un algorithme dissymétrique (F) et d'une clé secrète (Ks), et en portant cette valeur d'authentification sur le support ;
- procéder, lors de chaque utilisation du support, à une authentification de celui-ci par ledit distributeur dans un mode non connecté à l'organisme habilité, en effectuant un calcul par application à un algorithme (G) corrélé audit algorithme dissymétrique (F), d'une clé publique (Kp) associée à ladite clé secrète (Ks) et de la valeur d'authentification (VA) lue sur le support pour vérifier d'une part que la valeur d'authentification (VA) est compatible avec le numéro propre (Ns) et l'information (I), et d'autre part que la transaction ou le service demandé est compatible avec l'information (I) ;
- procéder périodiquement ou en fonction du type de transaction ou service, à une authentification du support à partir du distributeur dans un mode connecté à l'organisme habilité en effectuant tout d'abord une authentification du support par le distributeur ou l'organisme habilité qui vérifie que la valeur d'authentification (VA) lue sur le support est compatible avec le numéro propre (Ns) et l'information (I) et, si l'authentification est positive, en faisant confirmer par l'organisme habilité que le support possède encore des droits en fonction de l'état actuel dudit fichier puis, dans l'affirmative et si un changement de l'information (I) est nécessaire pour traduire l'état actuel des droits, en calculant, à partir du numéro propre (Ns) et d'une nouvelle information (I), une nouvelle valeur d'authentification (VA') au moyen de l'algorithme dissymétrique (F) et de la clé secrète (Ks), et en portant cette nouvelle valeur sur le support.

2. Procédé selon la revendication 1, dans lequel l'algorithme (G) corrélé à l'algorithme dissymétrique (F) comprend un algorithme (F^{-1}) inverse de celui-ci et, lors de chaque utilisation du support, on procède à ladite authentification en calculant avec cet algorithme le numéro propre (Ns) et l'information (I) relatifs au support à partir de la valeur d'authentification (VA) lue sur celui-ci, puis en vérifiant que le numéro propre (Ns) lu est identique à celui calculé et que l'information (I) calculée est cohérente en soi et compatible avec la transaction ou le service demandé.

3. Procédé selon la revendication 1, dans lequel ledit algorithme (G) corrélé à l'algorithme dissymétrique (F) est tel que ladite authentification nécessite la connaissance de l'information (I) et du numéro propre (Ns), l'information (I) étant soit portée sur le support, soit connue implicitement du distributeur, et, lors de chaque utilisation du support, on effectue ledit calcul en appliquant en outre à l'algorithme corrélé (G) le numéro propre (Ns) lu sur le support et l'information (I) lue sur le support ou connue implicitement.

4. Procédé selon l'une quelconque des revendications précédentes, dans lequel ladite information (I) inclut une date de référence permettant de calculer une date limite des droits attachés au support et, lors de chaque authentification, on vérifie si, au jour de la transaction ou du service demandé, la date limite des droits n'est pas dépassée.

5. Support de données ou dispositif comportant des moyens d'authentification pour permettre de vérifier qu'il émane bien d'un organisme habilité, ce support ou dispositif étant destiné à effectuer des transactions ou à permettre l'accès à un service ou à un lieu auprès d'un distributeur affilié audit organisme, l'organisme détenant, dans un fichier, le contenu des droits actuels attachés à chaque support, ce support portant un numéro propre (Ns) permettant de le distinguer parmi un ensemble de supports produits par ledit organisme, caractérisé en ce qu'il porte en outre une valeur d'authentification (VA) calculée par un algorithme dissymétrique (F) à partir d'une clé secrète (Ks), du numéro propre (Ns), et d'une information (I) définissant, en fonction du contenu dudit fi-

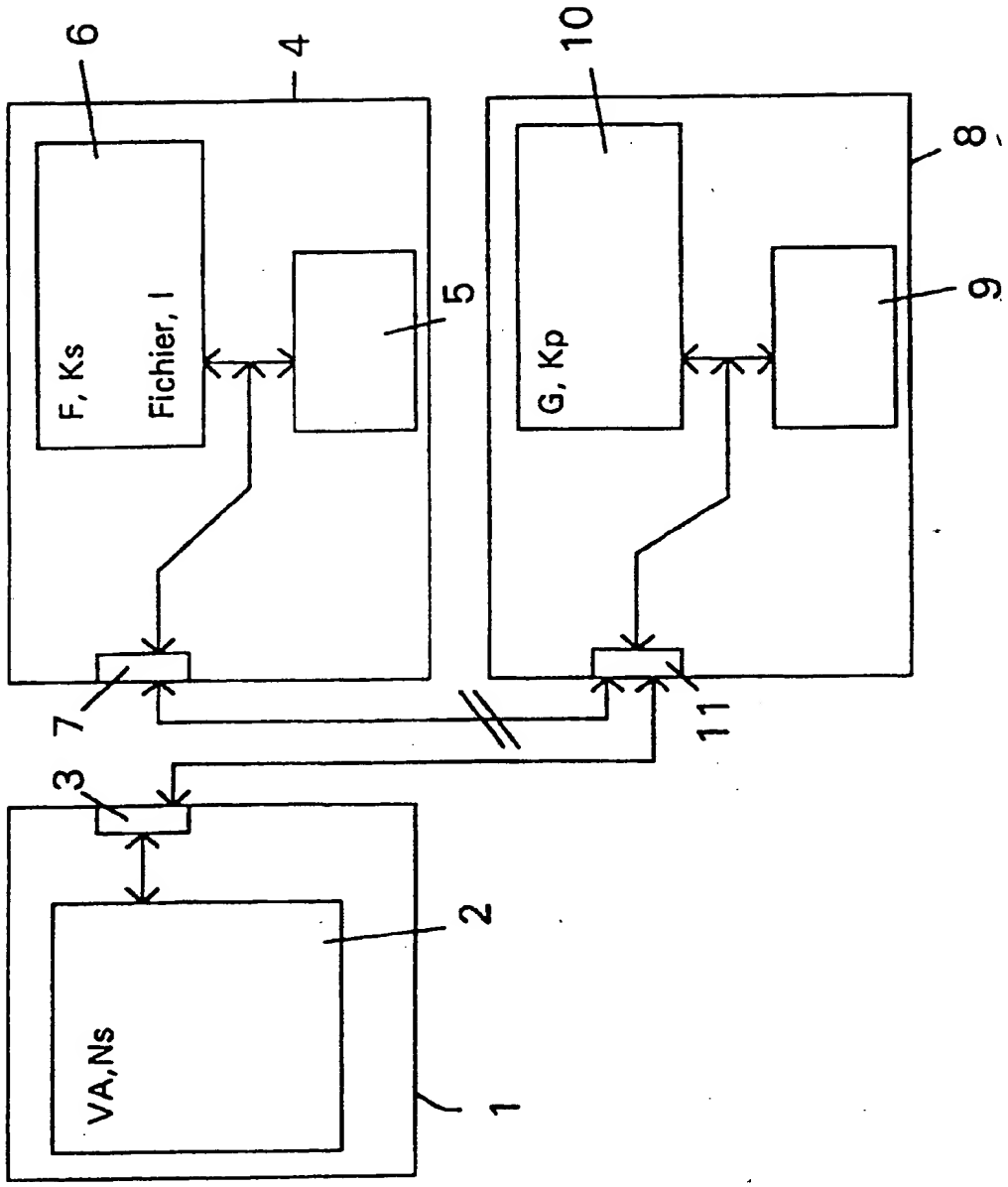
chier, les droits attachés à ce support.

6. Support selon la revendication 5, dans lequel l'algorithme dissymétrique (F) est tel que l'authentification du support nécessite la connaissance de l'information (I) et du numéro propre (Ns), l'information (I) étant spécifique à chaque support et portée sur celui-ci.

7. Support selon la revendication 5 ou 6, qui comprend un objet portatif équipé d'une mémoire électronique EEPROM dans laquelle est stockée ladite valeur d'authentification (VA).

8. Terminal agencé pour coopérer chez un distributeur avec un support de données ou dispositif selon l'un quelconque des revendications 5 à 7, caractérisé en ce qu'il comporte des moyens pour mémoriser un algorithme (G) corrélé audit algorithme dissymétrique (F) et une clé publique (Kp) associée à la clé secrète (Ks), et en ce qu'il est agencé pour effectuer un calcul par application à l'algorithme corrélé (G), de la clé publique (Kp) et de la valeur d'authentification (VA) lue sur le support pour vérifier d'une part que la valeur d'authentification (VA) est compatible avec le numéro propre (Ns) et l'information (I), et d'autre part que la transaction ou le service demandé est compatible avec l'information (I).

9. Dispositif central pour coopérer chez un organisme habilité avec un support de données ou dispositif selon l'une quelconque des revendications 5 à 7 caractérisé en ce qu'il comporte des moyens pour mémoriser ledit fichier, ledit algorithme dissymétrique (F) et ladite clé secrète (Ks), en ce qu'il est agencé pour confirmer que le support possède encore des droits en fonction de l'état actuel dudit fichier, et, dans l'affirmative et si un changement de l'information (I) est nécessaire pour traduire l'état actuel des droits, pour calculer, à partir du numéro propre (Ns) et d'une nouvelle information (I), une nouvelle valeur d'authentification (VA') au moyen de l'algorithme dissymétrique (F) et de la clé secrète (Ks), et pour porter cette nouvelle valeur sur le support.


6
4
10
8
F, Ks
Fichier, I
5
G, Kp
9
7
11
3
2
VA,Ns
1

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numero de la demande
EP 95 40 0505

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.6)
Y	US-A-4 453 074 (S.B. WEINSTEIN) * abrégé; revendications; figures 1-5 *	1-9	G07F7/08
Y	EP-A-0 299 826 (SCHLUMBERGER INDUSTRIES) * abrégé; revendications; figures * * colonne 5, ligne 22 - colonne 6, ligne 46 *	1-9	
A	GB-A-2 078 410 (RACAL-TRANSCOM) * abrégé; revendications *	1-8	
A	WO-A-85 02927 (FAIRVIEW PARTNERS)		
A	FR-A-2 246 913 (GRETAG)		

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)
G07F

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	17 Mai 1995	DAVID, J

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)